

WHAT IS CLAIMED IS:

1. A method of generating encrypted packets comprising the steps of:

generating at least one second Ethernet packet comprising  
5 at least one first Ethernet packet and at least one address associated with at least one security association;

extracting the at least one address and the at least one first Ethernet packet from the at least one second Ethernet packet;

10 retrieving at least one security association from at least one data memory according to the extracted at least one address; and

encrypting at least a portion of the extracted at least one first Ethernet packet according to the retrieved at least  
15 one security association.

2. The method of claim 1 wherein the generating step comprises generating an outer Ethernet header and another header.

3. The method of claim 1 wherein the another header  
20 comprises the at least one address.

4. The method of claim 3 wherein the outer Ethernet header comprises an Ethernet address of a security processor.

5. The method of claim 4 wherein the outer Ethernet header comprises a Broadcom Ethernet type field.

25 6. The method of claim 5 wherein a first byte of the another header comprises a zero.

7. The method of claim 6 wherein second, third and

fourth bytes of the another header comprise the at least one address.

8. The method of claim 7 wherein the at least one address comprises a lower 22 bits of the second, third and  
5 fourth bytes.

9. The method of claim 1 wherein the extracting step comprises determining whether an Ethernet type field from the at least one second Ethernet packet comprises a Broadcom Ethernet type.

10 10. The method of claim 9 wherein the extracting step comprises determining whether a first byte following an Ethernet type field from the at least one second Ethernet packet is set to a zero.

11. The method of claim 10 wherein the extracting step  
15 comprises extracting an address from second, third and fourth bytes following an Ethernet type field from the at least one second Ethernet packet.

12. The method of claim 11 wherein the extracting step  
20 comprises extracting an address from the lower 22 bits of second, third and fourth bytes following an Ethernet type field from the at least one second Ethernet packet.

13. The method of claim 12 wherein the retrieving step comprises retrieving the at least one security association from a data memory in a security processor.

25 14. The method of claim 13 wherein the encrypting step comprises using an encryption key associated with the at least one security association.

15. The method of claim 13 wherein the encrypting step comprises using an encryption algorithm defined by the at least one security association.

5 16. The method of claim 1 wherein the extracting step comprises determining whether an Ethernet address from the at least one second Ethernet packet matches an Ethernet address of a security processor.

10 17. A method of generating encrypted packets by processing at least one second Ethernet packet comprising at least one first Ethernet packet and at least one address associated with at least one security association, the method comprising the steps of:

15 extracting the at least one address and the at least one first Ethernet packet from the at least one second Ethernet packet;

retrieving at least one security association from at least one data memory according to the extracted at least one address; and

20 encrypting at least a portion of the extracted at least one first Ethernet packet according to the retrieved at least one security association.

25 18. The method of claim 17 wherein the extracting step comprises determining whether an Ethernet type field from the at least one second Ethernet packet comprises a Broadcom Ethernet type.

19. The method of claim 17 wherein the extracting step comprises determining whether a first byte following an Ethernet type field from the at least one second Ethernet packet is set to a zero.

20. The method of claim 17 wherein the extracting step comprises extracting an address from second, third and fourth bytes following an Ethernet type field from the at least one second Ethernet packet.

5        21. The method of claim 17 wherein the extracting step comprises extracting an address from the lower 22 bits of second, third and fourth bytes following an Ethernet type field from the at least one second Ethernet packet.

10       22. The method of claim 17 wherein the retrieving step comprises retrieving the at least one security association from a data memory in a security processor.

23. The method of claim 17 wherein the encrypting step comprises using an encryption key associated with the at least one security association.

15       24. The method of claim 17 wherein the encrypting step comprises using an encryption algorithm defined by the at least one security association.

20       25. The method of claim 17 wherein the extracting step comprises determining whether an Ethernet address from the at least one second Ethernet packet matches an Ethernet address of a security processor.

26. A method of generating packets to be encrypted comprising the steps of:

25       generating at least one first Ethernet packet;  
         associating at least one security association with the at least one first Ethernet packet;  
         identifying at least one address associated with the at least one security association; and

generating at least one second Ethernet packet comprising the at least one address and the at least one first Ethernet packet.

5        27. The method of claim 26 wherein the generating step comprises generating an outer Ethernet header comprising an address of a security processor.

10       28. The method of claim 26 wherein the generating step comprises generating an outer Ethernet header and another header.

29. The method of claim 28 wherein the outer Ethernet header comprises an Ethernet address of a security processor.

30. The method of claim 28 wherein the outer Ethernet header comprises a Broadcom Ethernet type field.

15       31. The method of claim 28 wherein the another header comprises the at least one address.

32. The method of claim 28 wherein a first byte of the another header comprises a zero.

20       33. The method of claim 28 wherein second, third and fourth bytes of the another header comprise the at least one address.

34. The method of claim 28 wherein the at least one address comprises a lower 22 bits of the second, third and fourth bytes.

25       35. The method of claim 26 further comprising the steps of:

receiving data to be sent over an Ethernet network; and  
incorporating the data into the at least one first  
Ethernet packet.

5        36. The method of claim 26 further comprising the step  
of transmitting the at least one second Ethernet packet to at  
least one security processor.

10       37. A security processor for generating encrypted  
packets by processing at least one second Ethernet packet  
comprising at least one first Ethernet packet and at least one  
address associated with at least one security association,  
comprising:

15       at least one data memory for storing at least one  
security association;

at least one Gigabit MAC for receiving at least one  
second Ethernet packet;

20       at least one processor, connected to receive at least a  
portion of the at least one second Ethernet packet from the at  
least one Gigabit MAC, for

extracting at least one address from the at  
least one second Ethernet packet; and

25       retrieving at least one security association  
from the at least one data memory according to the  
extracted at least one address; and

at least one encryption processor, connected to the at  
least one processor, for encrypting at least a portion of the  
at least one first Ethernet packet according to the retrieved  
at least one security association.

30

38. The security processor of claim 37 wherein the at  
least one second Ethernet packet comprises an outer Ethernet  
header and another header and the another header comprises the  
at least one address.

39. The security processor of claim 37 wherein the at least one encryption processor comprises at least one IPsec processor.

5

40. The security processor of claim 37 wherein the security processor is an integrated circuit.

41. An Ethernet controller comprising:

10

at least one processor for:

generating at least one TCP/IP packet;

associating at least one security association with the at least one TCP/IP packet; and

15

identifying at least one address associated with the at least one security association; and

at least one Gigabit MAC for generating at least one Ethernet packet comprising the at least one TCP/IP packet and the at least one address.

20

42. The Ethernet controller of claim 41 wherein the at least one Ethernet packet comprises an outer Ethernet header and another header and the another header comprises the at least one address.

25

43. The Ethernet controller of claim 41 wherein the Ethernet controller is an integrated circuit.

44. A method of generating packets to be encrypted comprising the steps of:

30

generating data to be sent securely over a packet network;

identifying at least one security association associated with the data;

identifying at least one address associated with the at

least one security association;

generating at least one packet comprising the at least one address and the data.

45. A method of generating encrypted packets by  
5 processing at least one packet comprising data to be sent securely over a packet network and at least one address associated with at least one security association, the method comprising the steps of:

10 extracting the at least one address and the data from the at least one packet;

retrieving at least one security association from at least one data memory according to the extracted at least one address; and

15 encrypting at least a portion of the extracted data according to the retrieved at least one security association.

46. A method of preparing packets for encryption comprising the steps of:

identifying encryption information associated with at least one packet;

20 generating at least one header comprising the encryption information;

appending the at least one header to the at least one packet; and

25 sending the appended at least one header and the at least one packet to a security processor.

47. The method of claim 46 wherein the encryption information comprises flow information.

30 48. The method of claim 46 wherein the encryption information comprises security association information.



49. The method of claim 46 wherein the encryption information comprises an address of a security association.

50. A method of generating encrypted packets comprising the steps of:

5       extracting encryption information from at least one header appended to at least one packet;

      retrieving encryption association information from at least one data memory according to the extracted encryption information; and

10       encrypting the at least one packet according to the retrieved encryption association information.

51. The method of claim 50 wherein the encryption information comprises flow information.

15

52. The method of claim 50 wherein the encryption information comprises security association information.

53. The method of claim 50 wherein the encryption  
20 information comprises an address of a security association.